I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

Data Breach Notification Legislation: Recent Developments

JULIE A. HEITZENRATER*

ABSTRACT: As data breaches continue to make news, state legislators continue to introduce new laws to protect consumers even as the federal government fails to provide unifying federal legislation. Recently, several states with no pre-existing data breach laws passed or initiated legislation. Other states have passed or initiated legislation broadening the definition of personal information (medical and biometric), legislating liability of retailers to financial institutions, forbidding any storage of PIN numbers and magnetic stripe data after processing an access card transaction, requiring disclosure to a government agency in addition to affected consumers, and requiring encryption of personal data. In addition to the added consumer protection provided by these laws, businesses are spending more on security, perhaps in reaction to this legislation. Overall, consumer protection from the potential effects of a data breach appears to be increasing rather than decreasing.

* The author is a 2009 Juris Doctor candidate at The Ohio State University Moritz College of Law. She received a B.S. in Metallurgical Engineering and Materials Science from Carnegie Mellon University in 1988.

I. INTRODUCTION

It has often been said, "The more things change, the more they stay the same." This is an apt statement for describing the status of both data breach occurrences and data breach legislation. The Identity Theft Research Center 2007 Data Breach Statistics indicated that well over 127,000,000 records were exposed in 446 data breach incidents in 2007,[1] and the Open Security Foundation reported that well over 83 million more were compromised in 2008.[2] In 2007, a data breach at TJX, the parent company of T.J. Maxx and Marshall's, revived both legislative and public interest in this subject.[3] Hackers obtained close to 100 million credit card numbers and thousands of driver's licenses and social security numbers.[4]

State legislatures continue to enact and modify data breach laws as the federal government remains unable to pass any legislation.[5] Modifications to existing state laws recently enacted or considered include: broadening the definition of personal information to include medical and biometric data, legislating liability of retailers to financial

---

[1] IDENTITY THEFT RESOURCE CTR., 2007 DATA BREACH STATS. 16 (2008), http://idtheftmostwanted.org/ITRC%20Breach%20Stats%20Report%202007.pdf. The total number of records exposed in the published incidents compiled by the Center was 127,725,343. *Id.* This is a conservative number as the number of records exposed was unavailable for many of the incidents. *Id.*

[2] OPEN SECURITY FOUNDATION, DATA LOSS DATABASE– 2008 YEARLY REPORT 1 (2009), http://datalossdb.org/yearly_reports/dataloss-2008.pdf. The total number of records exposed in the published incidents compiled by the Foundation was 83,448,112. *Id.* This is a conservative number as the number of records exposed was unavailable for many of the incidents. *Id.*

[3] *Hi-Tech Heist*, CBS NEWS, Nov. 25, 2007, http://www.cbsnews.com/stories/2007/11/21/60minutes/main3530302.shtml.

[4] *Id.* The Federal Trade Commission brought suit against TJX for violation of the Federal Trade Commission Act for failure to provide adequate security for their customers' personal information, which resulted in a settlement requiring TJX to retain independent, third-party security auditors to assess their security programs on a biennial basis for the next twenty years. Press Release, Federal Trade Commission, Agency Announces Settlement of Separate Actions Against Retailer TJX and Data Brokers Reed Elsevier and Seisint for Failing to Provide Adequate Security for Consumers' Data (Mar. 27, 2008), *available at* http://www.ftc.gov/opa/2008/03/datasec.shtm.

[5] For background information on pending federal legislation, see Michael E. Jones, Note, *Data Breaches: Recent Developments in the Public and Private Sectors*, 3 ISJLP 555, 570–74 (2007).

institutions, forbidding any storage of PIN numbers and magnetic stripe data after processing an access card transaction, requiring notice to a government agency in addition to affected consumers when a breach occurs, and requiring encryption.

While state legislatures are busily working on these issues, federal legislators who promised action after the 2006 elections have yet to pass any legislation.[6] The data breach bills continue to languish as Congress cannot agree on which provisions should be included.[7] No doubt, the ever-increasing and constantly changing patchwork of state laws continue to complicate Congress's efforts.

The positive for consumers in this situation is that their data is likely becoming more secure even without federal legislation. More new state laws are being passed and existing state laws are being strengthened. Moreover, as data breach costs continue to rise, businesses are beefing up security in order to avoid such costly incidents.[8]

II. STATE LEGISLATION

State data breach notification laws generally define three key elements: the trigger for providing consumers notice of a breach; the people or agencies to be notified; and the process for how that notification must take place. The main differences in breach notification laws from state to state usually involve the definition of when a mandatory notification is triggered.[9] In general, there are two types of triggers: acquisition-based triggers and risk-based triggers.[10] Acquisition-based triggers require consumer notification whenever personal data is reasonably believed to have been acquired by an unauthorized person but require no evidence that an unauthorized

---

[6] Brian Krebs, *Accountability Is Key Goal of Privacy Legislation*, WASHINGTONPOST.COM, Feb. 1, 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/02/01/AR2007020100748_pf.html.

[7] The variation in the legislation that has been introduced thus far is significant. *See* Part II, *infra*.

[8] *See* Doug Bartholomew, *2008 Spend[ing] on IT for IT to Jump 9.3 Percent*, BASELINEMAG.COM, Feb. 8, 2008, http://www.baselinemag.com/c/a/IT-Management/2008-Spend-on-IT-for-IT-to-Jump-93-Percent.

[9] Jones, *supra* note 5, at 561–62.

[10] *See id.* at 562–64.

person actually acquired the data.[11] Risk-based triggers allow for a risk assessment to determine whether any harm has or will be done to those whose records were potentially breached.[12] In these situations, notification is only necessary where the potential for harm exists.[13]

A. DATA BREACH NOTIFICATION

As of the end of 2008, forty-four states and the District of Columbia had data breach laws on the books.[14] Of these, five state data breach laws were newly enacted in 2008: Alaska, Iowa, South Carolina, Virginia, and West Virginia.[15] These laws and the bills proposed but not passed in the other states without statutes followed the general format of existing state data breach legislation. In addition, some incorporated provisions that were currently being added to existing legislation in other states. A little over half of the states with passed or proposed legislation in 2008 included risk-based triggers for notification– Alaska, Iowa, Kentucky, Mississippi and South Carolina; the rest included acquisition based triggers– Alabama, Missouri, Virginia, and West Virginia.[16] The history of the 2008 proposed legislation in the six states without enacted legislation is as follows:

---

[11] *Id.*

[12] *Id.*

[13] *Id.*

[14] NAT'L CONF. OF STATE LEGISLATORS, STATE SECURITY BREACH NOTIFICATION LAWS, http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm (last visited Feb. 7, 2009).

[15] H.R. 65, 25th Leg., 1st Sess. (Alaska 2008), *available at* http://www.legis.state.ak.us/basis/get_fulltext.asp?session=25&bill=HB65; S. File 2308, 82d Leg., 2d Sess. (Iowa 2008), *available at* http://coolice.legis.state.ia.us/Cool-ICE/default.asp?category=billinfo&Service=Billbook&ga=82&hbill=SF2308; S. 453, 2007–2008 Leg., 117th Sess. (S.C. 2007), *available at* http://www.scstatehouse.gov/cgi-bin/web_bh10.exe?bill1=&session=117 (must enter bill number); H.R. 1469, 2008 Leg., 2008 Sess. (Va. 2008), *available at* http://leg1.state.va.us/cgi-bin/legp504.exe?081+ful+HB1469ER; S. 340, 2008 Leg., 2008 Reg. Sess. (W. Va. 2008), *available at* http://www.legis.state.wv.us/bill_status/bills_history.cfm?year=2008&sessiontype=RS (must enter bill number in "Bill Quick Search" and choose desired version under "Bill Text").

[16] See text of bills cited in footnotes 15 and 17–20.

State	Status	Bill Number
Alabama[17]	Both died in committee in their house of origin (2/07)	H.B. 542, S. 382
Kentucky[18]	Passed in the House and died in committee in the Senate (3/26/08)	H.B. 553
Mississippi[19]	Passed in the House and died in committee in the Senate (3/18/08)	H.B. 1408
Missouri[20]	Died in committee (4/10/08)	H.B.1635
New Mexico	No bill pending	-----
South Dakota	No bill pending	-----

While federal data breach legislation is stalled in Congress, passage of state legislation appears to be working to create uniformity in consumer protection and the resulting requirements on businesses across the country. In fact, passage of data breach legislation in all states may aid businesses as well as consumers. While there will still be a patchwork of specific requirements, at least it will be clear that all

---

[17] H.R. 542, 2008 Leg., 2008 Reg. Sess. (Ala. 2007), *available at* http://alisondb.legislature.state.al.us/acas/ACTIONViewFrame.asp?TYPE=Instrument&INST=HB542&DOCPATH=searchableinstruments/2008RS/Printfiles/&PHYDOCPATH=//alisondb/acas/searchableinstruments/2008RS/PrintFiles/&DOCNAMES=HB542-int.pdf; S. 382, 2008 Leg., 2008 Reg. Sess. (Ala. 2007), *available at* http://alisondb.legislature.state.al.us/acas/ACTIONViewFrame.asp?TYPE=Instrument&INST=SB382&DOCPATH=searchableinstruments/2008RS/Printfiles/&PHYDOCPATH=//alisondb/acas/searchableinstruments/2008RS/PrintFiles/&DOCNAMES=SB382-int.pdf. History of the bills can be obtained through the Alabama Legislature website at http://alisondb.legislature.state.al.us/acas/ACASLogin.asp (choose "Regular Session 2008," "Bills," "Status," enter bill number).

[18] H.R. 553, 2008 Leg., 2008 Reg. Sess. (Ky. 2008), *available at* http://www.lrc.state.ky.us/record/08RS/HB553/bill.doc. History of the bill can be obtained through the Kentucky Legislature website, http://www.lrc.ky.gov/record/08RS/HB553.htm.

[19] H.R. 1408, 2008 Leg., Reg. Sess. 2008 (Miss. 2008), *available at* http://billstatus.ls.state.ms.us/documents/2008/pdf/HB/1400-1499/HB1408IN.pdf. History of the bill can be obtained through the Missippi Legislature website at http://billstatus.ls.state.ms.us/2008/pdf/history/HB/HB1408.xml.

[20] H.R. 1635, 94th Gen. Assem., 2d Reg. Sess. (Mo. 2008), *available at* http://www.house.mo.gov/billtracking/bills081/billpdf/intro/HB1635I.PDF. History of the bill can be obtained through the Missouri Legislature website at http://www.house.mo.gov/billtracking/bills081/bills/hb1635.htm.

states require some kind of notification in the event of a security breach.

B. BROADENING THE DEFINITION OF PERSONAL INFORMATION

Most state security breach statutes use similar definitions of personal information, implementing only minor modifications. Typically, the definition is an individual's first name or first initial and last name in combination with one of the following: a social security number; a driver's license or state ID number; or an account number combined with a security code, access code, or password that would permit access to an individual's financial account. However, as consumer awareness of data breach incidents increases and technology evolves, states are starting to look at expanding this definition.

Until recently, only Arkansas included medical information in its definition of personal information covered by its breach notification statute.[21] California followed suit in 2007. The California bill chaptered by the Secretary of State, amended the state's breach notification law by adding medical information and health insurance information to the state's definition of personal information.[22] In addition, prompted by recent reports of hospital employees prying into patient health records, California also enacted two laws in September, 2008 that require health facilities, clinics, hospices, and home health agencies to report unauthorized access of patient medical records to both the California Department of Public Health ("DPH") and to the affected individuals.[23] These laws also include substantial penalties for failure "to prevent or report unauthorized access, and

---

[21] ARK. CODE ANN. § 4-110-103(7)(D) (2008), *available at* http://www.arkleg.state.ar.us (select "Arkansas Code," then scroll down to "Arkansas Code," "Title 4", "Subtitle 7," "Chapter 110," "4-110-103").

[22] Assemb. 1298, 2007–2008 Leg., 2007–2008 Sess. § 4(1798.29)(e)(4)–(5) (Cal. 2008), *available at* http://www.leginfo.ca.gov/pub/07-08/bill/asm/ab_1251-1300/ab_1298_bill_20071014_chaptered.pdf.

[23] Assemb. 211, 2007–2008 Leg., 2007–2008 Sess. (Cal. 2008), *available at* http://www.leginfo.ca.gov/pub/07-08/bill/asm/ab_0201-0250/ab_211_bill_20080930_chaptered.pdf; S. 541, 2007–2008 Leg., 2007–2008 Sess. (Cal. 2008), *available at* http://www.leginfo.ca.gov/pub/07-08/bill/sen/sb_0501-0550/sb_541_bill_20080930_chaptered.pdf; Clark Stanton et al., *New Calif. Laws Strengthen Patient Privacy*, DWT.COM, Oct. 2008, http://www.dwt.com/practc/healthcr/bulletins/10-08_PatientPrivacy.htm.

even larger penalties on individuals who pry."[24] California has been a leader in breach notification law, so it will not be surprising if other states follow suit.[25] Kentucky, which currently has no data breach notification law at all, also included medical data in the definition of personal data in their proposed 2008 legislation.[26]

With the prospect of more frequent use of biometric data[27] to access private information in lieu of passwords and other more easily obtained codes, such data will likely be added to data breach law definitions of personal information in the future.[28] While personal data like account numbers and PINs are easy to change, fingerprints, retinas, and DNA cannot be changed following a breach; thus, the protection of such data is especially important.[29] Currently, only two states include this type of data in their definition of personal data subject to data breach notification. Nebraska protects "[u]nique biometric data, such as a fingerprint, voice print, or retina or iris image, or other unique physical representation,"[30] and Wisconsin protects "[t]he individual's deoxyribonucleic acid profile . . . [and] the individual's unique biometric data, including fingerprint, voice print, retina or iris image, or any other unique physical representation."[31] Iowa, which currently has no data breach notification law at all, included biometric data in the definition of personal data in their

---

[24] Stanton et al., *supra* note 23.

[25] Katherine Walsh, *CSO Disclosure Series: What California's New Medical Disclosure Law Means for the Rest of Us*, CSOONLINE.COM, Feb. 4, 2008, http://www.csoonline.com/article/print/217010.

[26] Ky. H.R. 553, *supra* note 18, at § 1(4)(h).

[27] Biometric data is data associated with human body characteristics "such as fingerprints, eye retinas and irises, voice patterns, facial patterns and hand measurements." SearchSecurity.com, Definitions, http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci211666,00.html (last visited Dec. 29, 2008).

[28] Peter Swire, Professor in Law and Judicial Administration, Michael E. Moritz College of Law, The Ohio State University, Remarks at ALI-ABA Course Privacy Law: Developments, Planning, and Litigation (Mar. 13, 2008).

[29] *Id.*

[30] NEB. REV. STAT. § 87-802(5)(e) (2008), *available at* http://uniweb.legislature.ne.gov/laws/statutes.php?statute=s8708002000.

[31] WIS. STAT. § 134.98(1)(b)(4)–(5) (2006–2007, Supp. 2008), *available at* http://www.legis.state.wi.us/statutes/Stat0134.pdf.

proposed 2008 legislation.[32] It is likely that more states will introduce legislation adding biometric data to their personal information definitions in the near future.

C. LIABILITY OF RETAILERS TO FINANCIAL INSTITUTIONS

The TJX breach has prompted a great deal of renewed activity on data breach laws in state legislatures. Two class action lawsuits have been filed by financial institutions against TJX to recover the costs incurred [33] when hackers stole tens of millions of credit card numbers.[34] Such costs can be substantial. TJX agreed to pay VISA $40.9 million to settle one of the suits.[35] Undoubtedly, this figure was lower than the actual costs incurred by the VISA financial institutions.

Legislators recognized the financial institutions' potential for harm when data is breached and, in 2007–2008, at least thirteen states introduced bills that provided a specific cause of action for financial institutions against third parties, especially retailers, for recovery of costs associated with a data breach. The costs included in the legislation were generally those associated with cancellation and reissuance of access devices (credit/debit cards), closure of accounts, opening or reopening of accounts, refunds for unauthorized transactions, and notification.[36] These bills took two forms. In the first type, the action was based on a data breach caused by violating a prohibition on retaining access card security code data, PIN verification code, or magnetic stripe data subsequent to the authorization of the transaction (as the retailer no longer needs this information and retention in their system subjects it to the risk of breach for a longer period of time than necessary). It should be noted

---

[32] Iowa S. File 2308, *supra* note 15, at § 1(11)(e).

[33] Erin Fonté, *Who Should Pay the Price for Identity Theft?*, 25 COMPUTER & INTERNET LAWYER 1, 2 (Feb. 2008), *available at* http://www.pillsburylaw.com/content/portal/publications/2008/2/2008128173310265/Identity%20Theft%20Computer%20&%20Internet%20Lawyer%20Fonte%20Feb%202008%2001-29-08.pdf.

[34] *Hi-Tech Heist*, *supra* note 3.

[35] Mark Jewell, *TJX, Visa Reach $40.9M Settlement for Data Breach*, USATODAY, Nov. 30, 2007, http://www.usatoday.com/money/industries/retail/2007-11-30-tjx-visa-breach-settlement_N.htm.

[36] *See, e.g.*, MINN. STAT. § 325E.64(3) (2007), *available at* https://www.revisor.leg.state.mn.us/statutes/?id=325E.64.

that the Payment Card Industry Standard that retailers are required by credit card companies to follow already includes the same prohibition on the retention of data addressed by the first type of bill. In the second type of bill, strict liability for the breach was imposed regardless of the cause of the breach.[37]

Thus far, only Minnesota has succeeded in passing such legislation.[38] The Minnesota law as well as legislation introduced in Alabama,[39] California,[40] Iowa,[41] Maryland,[42] New Jersey,[43] Texas,[44] and Wisconsin[45] proposed a cause of action based on the retention of

---

[37] PCI SECURITY STANDARDS COUNCIL, PAYMENT CARD INDUSTRY DATA SECURITY STANDARD 5 (Ver. 1.1, Sept. 2006), https://www.pcisecuritystandards.org/security_standards/pci_dss_download.html (required to select "I agree" and then download PDF; or to download directly—https://www.pcisecuritystandards.org/security_standards/download.html?id=pci_dss_v1-1.pdf).

[38] MINN. STAT. § 325E.64, *supra* note 36.

[39] Ala. H.R. 542, *supra* note 17, at § 4.

[40] Assemb. 779, 2007–2008 Leg., 2007–2008 Sess. (Cal. 2007), *available at* http://www.leginfo.ca.gov/pub/07-08/bill/asm/ab_0751-0800/ab_779_bill_20070914_enrolled.pdf. History of the bill can be obtained through the California Legislature website at http://www.leginfo.ca.gov/pub/07-08/bill/asm/ab_0751-0800/ab_779_bill_20080528_status.html.

[41] S. Study B. 3200, 82d Leg., 2008 Sess. (Iowa 2008), *available at* http://coolice.legis.state.ia.us/Cool-ICE/default.asp?Category=BillInfo&Service=Billbook&ga=82&hbill=SSB3200.

[42] H.R. 129, 2008 Leg., 425th Sess. § 2(14-3501) (Md. 2008), *available at* http://mlis.state.md.us/2008rs/bills/hb/hb0129f.pdf. History of the bill can be obtained through the Maryland Legislature website at http://mlis.state.md.us/2008rs/billfile/HB0129.htm.

[43] Assemb. 2270, 213th Leg., 2008–2009 Sess. § 3(12)(g) (N.J. 2008), *available at* http://www.njleg.state.nj.us/2008/Bills/A2500/2270_I1.PDF. History of the bill can be obtained through the New Jersey Legislature website http://www.njleg.state.nj.us/bills/billso001.asp (choose "Bill Number," enter bill number).

[44] H.R. 3222, 80th Leg., Reg. Sess. § 1(48.102)(e) (Tex. 2007), *available at* http://www.capitol.state.tx.us/tlodocs/80R/billtext/pdf/HB03222E.pdf. History of the bill can be obtained through the Texas Legislature website at http://www.capitol.state.tx.us/BillLookup/History.aspx?LegSess=80R&Bill=HB3222.

[45] Assemb. 745, 2007–2008 Leg., 2007–2008 Sess. § 1(100.545)(3) (Wis. 2007), *available at* http://www.legis.state.wi.us/2007/data/AB-745.pdf; S. 439, 2007–2008 Leg., 2007–2008 Sess. § 1(100.545)(3) (Wis. 2007), *available at*

access card security data, while bills introduced in Connecticut,[46] Illinois,[47] Massachusetts,[48]Michigan,[49] and Washington[50] proposed a strict liability cause of action. Most of this legislation failed to pass: Alabama (died in committee), Connecticut (provision removed from the bill), California (vetoed), Illinois (failed to pass before the session ended), Iowa (provision removed from the bill), Maryland (unfavorable committee report), Massachusetts (died in committee), Texas (died in committee), Washington (failed to pass before the session ended), and Wisconsin (failed to pass before the session ended).

Businesses, especially small ones, and some bankers protested that such laws would impose financial burdens[51] because they feared

---

http://www.legis.state.wi.us/2007/data/SB-439.pdf. Histories of the bills can be obtained through the Wisconsin Legislature website at http://nxt.legis.state.wi.us/nxt/gateway.dll?f=templates&fn=default.htm&d=billhist07&jd=top (enter bill number in the search box).

[46] Substitute S.B. 1089, 2007 Leg., 2007 Jan. Sess. § 2(1724.5)(d) (Conn. 2007), *available at* http://www.cga.ct.gov/2007/TOB/s/pdf/2007SB-01089-R04-SB.pdf. History of the bill can be obtained through the Connecticut Legislature website at http://www.cga.ct.gov/asp/cgabillstatus/cgabillstatus.asp?selBillType=Bill&bill_num=1089&which_year=2007&SUBMIT1.x=11&SUBMIT1.y=7.

[47] S. 1675, 95th Gen. Assem., 2007–2008 Sess. § 3 (Ill. 2007), *available at* http://ilga.gov/legislation/fulltext.asp?DocName=09500SB1675sam001&GA=95&SessionId=51&DocTypeId=SB&LegID=&DocNum=1675&GAID=9&Session=. History of the bill can be obtained through the Illinois Legislature website at http://ilga.gov/reports/static/95thStatus%20of%20Bills-Cumulative.pdf.

[48] H.R. 213, 2007 Leg., 185th Sess. § 4 (Mass. 2007), *available at* http://www.mass.gov/legis/bills/house/185/ht00pdf/ht00213.pdf. History of the bill can be obtained through the Massachusetts Legislature website at http://www.mass.gov/legis/185history/h00213.htm.

[49] S. 1022, 94th Leg., Reg. Sess. § 11(16) (Mich. 2008), *available at* http://www.legislature.mi.gov/documents/2007-2008/billintroduced/Senate/pdf/2008-SIB-1022.pdf. History of the bill can be obtained through the Michigan Legislature website at http://www.legislature.mi.gov/(S(eetarc452bovudu2ittuozzp))/mileg.aspx?page=getObject&objectName=2008-SB-1022.

[50] Substitute H.B. 2838, 60th Leg., 2008 Reg. Sess. § 1 (Wash. 2008), *available at* http://apps.leg.wa.gov/documents/billdocs/2007-08/Pdf/Bills/House%20Bills/2838-S.pdf (original bill required breach to be based on retention of access card security code data). History of the bill can be obtained through the Washington Legislature website at http://apps.leg.wa.gov/billinfo/summary.aspx?bill=2838&year=2007.

[51] Fonté, *supra* note 33, at 6.

that a substantial breach could put a retailer out of business.[52] Governor Schwarzenegger of California also agreed and vetoed a California bill, stating that, "[t]his bill attempts to legislate in an area where the marketplace has already assigned responsibilities and liabilities . . . ."[53] In vetoing the bill, Schwarzenegger sided with the Retailer's Association, Chamber of Commerce, and Banker's Association, [54] which argued that government intervention was unnecessary and overreaching as the industry was already regulated by Payment Card Industry Standards and retailers already paid these costs to the financial institutions as part of contractual "interchange fees" associated with processing a transaction.[55] Allowing recovery after a breach, they asserted, would amount to "double-dipping."[56]

Credit unions, on the other hand, were actively supporting such bills[57] and even wrote some of them.[58] They argued that the laws were needed because retailers were not following the Payment Card Industry Standards and fines and fees were not sufficient to encourage them to do so.[59] The credit unions contended that the government needed to step in and provide that incentive through data breach liability laws.[60]

---

[52] Katie Kuehner-Hebert, *Bank-CU Tactical Divide on Breach Liability Bills*, 173 AM. BANKER 5 (Mar. 14, 2008).

[53] Assemb. 779 Veto Message, 2007–2008 Leg., 2007–2008 Sess. (Cal. 2007), *available at* http://www.leginfo.ca.gov/pub/07-08/bill/asm/ab_0751-0800/ab_779_vt_20071013.html.

[54] Dan Kaplan, *Schwarzenegger Shoots Down Data-Protection Bill*, SC MAGAZINE, Oct. 15, 2007, http://www.scmagazineus.com/Schwarzenegger-shoots-down-California-data-protection-bill/article/57998.

[55] Kaplan, *supra* note 54; Kuehner-Hebert, *supra* note 52.

[56] Kuehner-Hebert, *supra* note 52.

[57] *Id.*

[58] Credit Union National Assoc., *Alabama League Introduces Data Security Legislation*, CUNA.ORG, Feb. 22, 2008, http://www.cuna.org/newsnow/archive/list.php?date=022108#34933; Credit Union National Assoc., *Maine League's Data Breach Bill Passes Committee*, CUNA.ORG, Feb. 25, 2008, http://www.cuna.org/newsnow/archive/list.php?date=022208#34956.

[59] Kuehner-Hebert, *supra* note 52.

[60] *Id.*

D. REPORTING BREACH TO A GOVERNMENT AGENCY

Only a few states require reporting a data security breach to a government agency. Hawaii requires a report to the Office of Consumer Protection only if over 1000 records are breached.[61] In New Hampshire, for businesses regulated by one of several state or federal agencies who possess the authority to regulate unfair or deceptive trade practices, notification must be made to those regulatory agencies; otherwise, notification to the attorney general is required.[62] Further, New Hampshire posts the notifications on the Internet.[63]

Indiana recently tried to pass similar legislation that would require notification of the state attorney general who would then post a list of breach notifications on the Internet.[64] The goal was to provide a central location for information on data breach incidents.[65] In the end, however, the amended Senate bill was stripped of the provision,[66] and the House accepted the Senate bill as amended.[67]

---

[61] HAW. REV. STAT. § 487N-2(f) (2007), *available at* http://www.capitol.hawaii.gov/hrscurrent/Vol11_Ch0476-0490/HRS0487N/HRS_0487N-0002.htm.

[62] N.H. REV. STAT. ANN. §§ 359-C:20(b), 358-A:3 (2007), *available at* http://www.gencourt.state.nh.us/rsa/html/XXXI/359-C/359-C-20.htm and http://www.gencourt.state.nh.us/rsa/html/xxxi/358-a/358-a-mrg.htm. Such agency notification must be made to the bank commissioner, the director of securities regulation, the insurance commissioner, the public utilities commissioner, the financial institutions and insurance regulators of other states, and federal banking and securities regulators. *Id.*

[63] Surveill@nce St@te, http://www.cnet.com/8301-13739_1-9865076-46.html (last visited Feb. 7, 2009).

[64] H.R. 1197, 115th Gen. Assem., 2d Reg. Sess. (Ind. 2008) (introduced), *available at* http://www.in.gov/legislative/bills/2008/IN/IN1197.1.html.

[65] Surveill@nce St@te, *supra* note 63.

[66] H.R. 1197, 115th Gen. Assem., 2d Reg. Sess. (Ind. 2008) (engrossed), *available at* http://www.in.gov/legislative/bills/2008/EH/EH1197.1.html.

[67] Bill Info, Digest of HB1197, http://www.in.gov/apps/lsa/session/billwatch/billinfo?year=2008&session=1&request=getBill&docno=1197#latest_info. It appears that the Indiana legislature was influenced by industry giants—Microsoft, AT&T, Verizon—who were lobbying against the bill. They asserted that the posting of the breaches would provide phishers and other online fraudsters with information to use as bait to gain individuals' personal information. They could send e-mails to potentially affected individuals containing a link to the attorney general's site as well as a link to a fraudulent site where consumers desiring to protect

Such legislation would prove very valuable in the fight to reduce data security breaches. Notification to a centralized agency would establish a consolidated database that could be used by consumers, security professionals, and government agencies. Consumers could use it to research data security when considering purchasing services;[68] security professionals could use it as an analytical tool;[69] and government agencies could use it to identify repeat offenders against whom enforcement actions should be taken.[70]

E. REQUIRING ENCRYPTION

While most state data security breach laws do not require notice to consumers when the data is encrypted, Nevada and Massachusetts require encryption for the electronic transmission of personal data.[71] Encryption is defined in Nevada as "the use of any protective or disruptive measure, including, without limitation, cryptography, enciphering, encoding or a computer contaminant." [72] In

---

themselves would be tricked into providing personal information. There appears to be little evidence that the concern is well founded as it does not appear that unscrupulous characters have used the New Hampshire site or various other consumer sites providing similar information to obtain information in order to commit identity theft. Surveill@nce St@te, *supra* note 63.

[68] CHRIS JAY HOOFNAGLE, *Security Breach Notification Laws: Views from Chief Security Officers*, *in* PRIVACY LAW: DEVELOPMENTS, PLANNING, AND LITIGATION – ALI-ABA COURSE OF STUDY MATERIALS 25, 31 (2008); Peter P. Swire, *A Theory of Disclosure for Security and Competitive Reasons: Open Source, Proprietary Software, and Government Systems*, 42 HOUS. L. REV. 1333, 1345 (2006).

[69] *Id.*

[70] *Id.*

[71] NEV. REV. STAT § 597.970 (2007), *available at* http://www.leg.state.nv.us/NRS/NRS-597.html#NRS597Sec970; 201 MASS. CODE REGS. 17.01 (2007) (implementing MASS. GEN. LAWS ch. 93H), *available at* http://www.mass.gov/?pageID=ocaterminal&L=4&L0=Home&L1=Consumer&L2=Privacy&L3=Identity+Theft&sid=Eoca&b=terminalcontent&f=reg201cmr17&csid=Eoca. Personal data includes first name or first initial and last name in combination with one or more of social security number, driver's license number or identification card number, and account number, credit card number, or debit card number, in combination with any required security code, access code or password that would permit access to the person's financial account. NEV. REV. STAT § 603A.040 (2007), *available at* http://www.leg.state.nv.us/NRS/NRS-603A.html#NRS603ASec040.

[72] NEV. REV. STAT. § 205.4742 (2007), *available at* http://www.leg.state.nv.us/NRS/NRS-205.html#NRS205Sec4742.

Massachusetts, encryption is defined as "transformation of data through the use of a 128-bit or higher algorithmic process, or other means or process approved by the Office of Consumer Affairs and Business Regulation that is at least as secure as an algorithmic process, into a form in which there is a low probability of assigning meaning without use of a confidential process or key."[73]

Identity theft bills with encryption requirements in addition to data breach notification requirements were included in proposed 2008 legislation in Michigan[74] and Washington.[75] The Michigan bill required encryption "in conformity with current industry-standard encryption methods and capabilities" for stored information.[76] The Washington bill required "encryption practices that are generally accepted by the industry" for transmitted and stored information.[77]

The TJX debacle has demonstrated that the quality of the encryption is just as important as its presence.[78] TJX used encryption based on the Wired Equivalent Privacy ("WEP") model.[79] However, this encryption code has been shown to have weaknesses that made it possible for hackers to determine the network's wireless encryption key.[80] The Wi-Fi Protected Access ("WPA") model, which was available at the time, is a much more secure system that, if used, could

---

[73] 201 MASS. CODE. REGS. 17.02 (2007) (implementing MASS. GEN. LAWS ch. 93H), *available at* http://www.mass.gov/?pageID=ocaterminal&L=4&L0=Home&L1=Consumer&L2=Privacy&L3=Identity+Theft&sid=Eoca&b=terminalcontent&f=reg201cmr17&csid=Eoca.

[74] Mich. S. 1022, *supra* note 49.

[75] H.R. 2574, 60th Leg., 2008 Reg. Sess. § 1 (Wash. 2008), *available at* http://apps.leg.wa.gov/billinfo/summary.aspx?bill=2574&year=2007. History of the bill can be obtained through the Washington Legislature website at http://apps.leg.wa.gov/billinfo/summary.aspx?bill=2838&year=2007.

[76] Mich. S. 1022, *supra* note 49, at § 11(1)(E).

[77] Wash. H.R. 2574, *supra* note 75, at § 1(2). In addition, a bill in Indiana requiring encryption on portable electronic devices, such as laptops and flash drives, has passed both the House and Senate. The bill does not define encryption. Ind. H.R. 1197, *supra* note 66.

[78] Mike Chapple, *Lessons Learned from TJX: Best Practices for Enterprise Wireless Encryption*, SEARCHSECURITY.COM, Dec. 12, 2007, http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1286596,00.html.

[79] *Id.*

[80] *Id.*

have potentially averted the breach.[81] However, with the ever-changing encryption technology and hackers constantly learning how to overcome the best way to mandate encryption is still a question to be answered. Mandating a specific technology will not work because improvements to technology usually outpace the ability of the legislature to change the laws.[82] This is a potential problem with the Massachusetts regulation. Conversely, the vague language of the Nevada law ("protective or disruptive measure"), the Michigan bill ("current industry-standard encryption"), and the Washington bill ("encryption practices that are generally accepted by the industry") does not really define what level of encryption is required[83] and thus, these laws are probably not effective mandates. It seems likely, however, that the exception for encrypted data in most breach notification laws, and the increasing costs resulting from data breach incidents will incentivize business and drive the market to the use of encryption even absent legislation.

III. FEDERAL LEGISLATION

The variety of state legislation concerning data security breaches in combination with the amount of personal data that is transmitted across state lines cries out for overarching federal legislation. Nonetheless, Congress has been very slow in enacting federal legislation.[84] When Massachusetts Representative Barney Frank became chairman of the House Financial Services Committee at the beginning of 2007, his interest in data privacy indicated that federal legislation might make some headway in the House.[85] Yet, although three data breach bills were reported out of committee in the Senate in 2007,[86] the House bills did not advance. The first bill reintroduced in

---

[81] *Id.*

[82] Correy E. Stephenson, *States Push Through Data Breach Laws*, LAWYERS USA, Mar. 10, 2008.

[83] *Id.*

[84] For background information on pending laws, see Jones, *supra* note 5, at 570–74.

[85] Krebs, *supra* note 6.

[86] Notification of Risk to Personal Data Act of 2007, S. 239, 110th Cong. (2007); Personal Data Privacy and Security Act of 2007, S. 495, 110th Cong. (2007); Identity Theft Protection Act, S. 1178, 110th Cong. (2007) were reported out of committee in 2007. Text and history of federal legislation is available at http://www.thomas.gov/bss/110search.html (enter bill number).

the Senate in 2008 was Senator Feinstein's bill (S. 239), which seemed to have the most support the previous year.[87] However, there was no progress on this bill after it was placed on the Senate calendar on May 31, 2007.[88] On January 18, 2008, Senator Feinstein sent a letter to Senate Majority Leader Reid requesting his assistance in moving the bill forward, but evidently to no avail.[89] Other federal bills have met similar fates– none were passed into law before the 110th Congress convened at the end of 2008.

The proposed federal bills had as many variations as the state legislation. Depending on the bill, the trigger for breach notification may be either acquisition-based or risk-based and reporting to a government agency may or may not be included. Senate Bills 239 and 495 included safe harbor provisions that amounted to a risk-based trigger. These bills also proposed acquisition-based notification of the Secret Service for breaches involving more than 10,000 individuals' data; when the breached database contains the information of more than 1,000,000 individuals nationwide; where the breached database is owned by the federal government; or where the breached database contains information of employees of the government involved in national security or law enforcement.[90] Alternatively, H.R. 836 (introduced in February 2007) did not address notification of individuals but required risk-based notification of either the Secret Service or the Federal Bureau of Investigation for breaches involving more than 10,000 individuals' data; where the breached database is owned by the federal government; or where the breached database contains information of employees of the government involved in national security or law enforcement.[91] Taking a third approach, S. 1178 (reported out of committee and placed on the Senate calendar in December 2007) had a risk-based trigger for individual notification of consumers but an acquisition-based trigger for notification of the

---

[87] *Id.*; *see generally* Notification of Risk to Personal Data Act of 2007, S. 239, 110th Cong. (2007).

[88] History of the bill can be obtained at http://www.thomas.gov/bss/110search.html (enter bill number).

[89] Press Release, Sen. Dianne Feinstein, Senator Feinstein Asks Senate Majority Leader to Bring Up Legislation to Protect Consumers from Identity Theft (Jan. 18, 2008).

[90] Notification of Risk to Personal Data Act of 2007, S. 239, 110th Cong. §§ 3(b), 7 (2007); Personal Data Privacy and Security Act of 2007, S. 495, 110th Cong. §§ 312(b), 316 (2007).

[91] Cyber-Security Enhancement and Consumer Data Protection Act of 2007, H.R. 836, 110th Cong. § 7 (2007).

Federal Trade Commission ("FTC") and all consumer reporting agencies.[92] The FTC would be required to post notice of the data breach on its website if the breach involved more than 1000 individuals' data.[93] Finally, H.R. 958 (introduced in February 2007) required acquisition-based notification of both individuals and the FTC.[94]

There were some indications in 2008, such as Senator Feinstein's letter to Senator Reid, that congressional interest in passing a data breach law was going to be renewed. The federal relations manager for security provider Symantec indicated that there was a flurry of activity in the House committees in an effort to catch up to the Senate.[95] For example, H.R. 4791, The Federal Agency Data Protection Act[96] (which would have codified the breach notification guidelines for federal agencies that were put in place in 2007 by the Office of Management and Budget) passed in the House and was sent to the Senate in June of 2008.[97] However, this bill, like the others, failed to pass before the legislature convened.

There seem to be several factors that have and will continue to contribute to the slow movement of the federal data breach legislation. First, the three proposed Senate bills were sent to two different committees and the two proposed House bills were sent to two different committees.[98] This makes it difficult to consolidate the bills and form a consensus on the requirements that should be in the

---

[92] Identity Theft Protection Act, S. 1178, 110th Cong. § 3(a), (c) (2007).

[93] *Id.* at § 3(a)(2).

[94] Data Accountability and Trust Act, H.R. 958, 110th Cong. § 3(a) (2007).

[95] Greg Piper, *Election Means Data Security Bills Must Wrap by Summer, Symantec Says*, 9 WASH. INTERNET DAILY, Jan. 28, 2008.

[96] *Id.*

[97] *Id.*; Federal Agency Data Protection Act, H.R. 4791, 110th Cong. (2007); *see generally* Jones, *supra* note 5, at 568–70.

[98] S. 239 and S. 495 were sent to the Committee on the Judiciary. S. 1178 was sent to the Committee on Commerce, Science, and Transportation. H.R. 958 was sent to the Committee on Energy and Commerce Subcommittee on Commerce, Trade, and Consumer Protection, and H.R. 836 was sent to the Committee on the Judiciary Subcommittee on Crime, Terrorism, and Homeland Security. The Library of Congress– Thomas Home, http://www.thomas.gov/bss/110search.html (last visited Feb. 7, 2009) (enter bill number, choose the version of the bill, choose "Bill Summary & Status File," and choose "Committees"). History of these bills is also available at this website.

federal legislation. Second, as 2008 was an election year, significant movement did not occur.[99] Third, the current congressional focus on economic issues and the Iraq War will likely overshadow breach notification legislation in the near term. However, the slow progress on federal legislation may not be harming consumers. The patchwork of state laws is a problem for businesses, not for consumers. Compared to the bills that have passed congressional committees to date, most consumers are receiving as much and sometimes more protection than they would receive if federal legislation were passed.

IV. ARE THE FINANCIAL AND REPUTATIONAL COSTS ASSOCIATED WITH DATA BREACH NOTIFICATION LEADING TO BETTER SECURITY?

As Carol DiBattiste, Chief Privacy Officer for Choicepoint, the company that experienced one of the first highly publicized data breaches in 2005, has stated in regard to data breaches, "[p]reventing is better than reacting."[100] In 2007, the cost of a data breach increased to $197 per record, an 8% increase over 2006 and a 43% increase over 2005.[101] Lost business accounted for 65% of these costs showing that the breaking of trust, while intangible in some respects, still has definite cost implications.[102] These increases were likely at least partially driven by the costs of compliance with new state data breach notification laws and the now common negative press and resulting loss of good will when a breach occurs.[103] As businesses continue to feel increased impacts from these laws, it appears that they are beginning to invest more proactively in security in order to avoid the financial and reputational costs associated with such breaches.

---

[99] Elayne Demby, *All Quiet on the Federal Front*, 13 COLLECTIONS & CREDIT RISK 28 (Feb. 2008).

[100] Carol DiBattiste, Chief Privacy Officer, Choicepoint, Remarks at ALI-ABA Course Privacy Law: Developments, Planning, and Litigation (Mar. 13, 2008).

[101] PONEMON INSTITUTE, 2007 ANNUAL STUDY: U.S. COST OF A DATA BREACH: UNDERSTANDING FINANCIAL IMPACT, CUSTOMER TURNOVER, AND PREVENTATIVE SOLUTIONS 2 (2007), http://www.vontu.com/uploadedfiles/global/Ponemon-Cost-of-a-Data-Breach-2007.pdf.

[102] *Id.* at 2, 17.

[103] *See id.* at 17; SAMUELSON LAW, TECH. & PUB. POL'Y CLINIC, UNIVERSITY OF CALIFORNIA-BERKELEY SCHOOL OF LAW, SECURITY BREACH NOTIFICATION LAWS: VIEWS FROM CHIEF SECURITY OFFICERS 12–13 (Dec. 2007), http://www.truststc.org/pubs/310/cso_study.pdf.

Businesses have begun to consider information security risk in a more strategic manner.[104] Increased regulation and legislation, and more awareness by upper management of the costs and exposure resulting from data breaches, are driving this change in thinking.[105] Forty-nine percent of businesses indicated that information security was one of their top two information technology priorities for 2008.[106] In addition, the federal government appeared to be following the private sector's lead. George W. Bush's fiscal 2009 budget request called for a 10% increase in government information technology security spending, for a total of $7.3 billion.[107]

Although there does not appear to be agreement as to how much is currently spent in the private sector on information security, security spending has been increasing and was expected to continue to increase in 2008. [108] Supporting this conclusion was the announcement by IBM that it committed to spend $1.5 billion on security research and was offering a one-stop program addressing PCI standards.[109] It seems unlikely that a company like IBM considered investing this amount of money if security spending was not expected to increase.

In addition, passage of the proposed state data breach financial liability and mandatory encryption laws will provide incentives for proactive, as opposed to reactive, security spending. And, businesses are also realizing that exceptional security practices can be a selling point that can increase business. [110] Encryption and data loss

---

[104] Bartholomew, *supra* note 8.

[105] *Id.*

[106] *Id.*

[107] Wyatt Kash, *Spending for IT security Gains Ground in 09 Budget*, GOV'T COMPUTER NEWS, Feb. 7, 2008, http://www.gcn.com/online/vol1_no1/45798-1.html.

[108] *See* Computing Technology Industry Assoc., *Information Security Spending on the Rise, CompTIA Survey Reveals*, COMPTIA CERTIFICATION NEWS & SPECIAL INFO., Oct. 9, 2007, http://certification.comptia.org/news/get_news.aspx?prid=1286; Peter Piazza, *Risks from Remote Workers Spur Security Spending*, ENTERPRISE SEC. TODAY, Mar. 12, 2008, http://www.enterprise-security-today.com/story.xhtml?story_id=0320013Q0MHS; Symantec, *Financial Institutions Spending More on Security, Governance*, Oct. 9, 2007, http://www.symantec.com/business/news/article.jsp?aid=in_100907_finance_spending.

[109] Robert Westervelt, *IBM to Boost Spending, Push PCI DSS Program*, SEARCHSECURITY.COM, Nov. 1, 2007, http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1280517,00.html.

[110] Nathan Conz, *Selling Security*, INS. & TECH. 31, Mar. 1, 2008.

prevention solutions are the top two responses following a breach.[111] Therefore, it is likely that businesses will start investing proactively in these areas.

While no concrete data is available to show just how much proactive security spending is occurring as a result of the implementation of data breach notification laws, all factors indicate that there has been a shift in the direction of proactivity. While more spending does not necessarily equate to better security, it certainly cannot hurt and probably indicates that the overall protection of consumers' personal data is improving.

V. CONCLUSION

Although large data breaches continue to occur, consumers should expect increased protection against data breaches in coming years. Legislation will likely be in the form of state legislation as opposed to federal legislation. Although the Obama administration lists on its agenda a goal to "[s]trengthen privacy protections for the digital age and harness the power of technology to hold government and business accountable for violations of personal privacy,"[112] the economic issues facing the country in 2009 will likely dominate the federal landscape. However, state legislation is likely to continue. Potential passage of state laws allowing financial liability for data breach (like Minnesota's), requiring disclosure to a government agency and subsequent posting of data breaches, and including medical and biometric data in the definition of personal information will give businesses more incentive to proactively invest in information technology security. Even absent these new laws, private sector and government proactive spending on security has increased and will continue to increase as a result of the increased financial and reputational costs associated with breaches. While progress may seem slow to consumers who have been victims of a data breach, every piece of new legislation and every dollar of increased security spending will hopefully make data breaches an uncommon occurrence in the future.

---

[111] PONEMON INSTITUTE 2007 ANNUAL STUDY, *supra* note 101, at 3.

[112] The White House, The Agenda – Technology, http://www.whitehouse.gov/agenda/technology (last visited Feb. 7, 2009).